UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/734,028	12/11/2003	Blair B. Dillaway	MSFT-2795/305124.1	2338

41505 7590 07/21/2009

WOODCOCK WASHBURN LLP (MICROSOFT CORPORATION)
CIRA CENTRE, 12TH FLOOR
2929 ARCH STREET
PHILADELPHIA, PA 19104-2891

EXAMINER	
JOHNSON, CARLTON	

ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
07/21/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/734,028	DILLAWAY ET AL.	
	Examiner	Art Unit	
	CARLTON V. JOHNSON	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 March 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *2-4,7-12,14,16,18-21,23 and 25-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *2-4,7-12,14,16,18-21,23 and 25-36* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responding to application amendments file on 3-24-2009.

2. Claims **2 - 4, 7 - 12, 14, 16, 18 - 21, 23, 25 - 36** are pending. Claims **2 - 4, 7 - 12, 14, 16, 18 - 21, 23, 25 - 30** have been amended. Claims **31 - 36** are new. Claims **1, 5, 6, 13, 15, 17, 22, 24** have been cancelled. Claims **19, 30, 31** are independent. This application was filed on 12-11-2003.

Response to Arguments

3. Applicant's arguments have been fully considered but they were not persuasive.

3.1 The 112 rejection has been withdrawn due to amendments.

3.2 Applicant argues that the referenced prior art does not disclose, *a two step process for attestation; two pre-attestation messages. (Remarks Page 13, 15)*

Specification in paragraph [0053] discloses that the can-attest message (request) can have any format and contain any relevant information such as identification of first entity. Specification in paragraph [0055] discloses that the attestation-wanted message (response) contains the requirements for the attestation. Yan prior art discloses for claims 31, 18, 19, 30, 31, two message flows used for the initiation and completion of attestation between two entities. The two message-flows (paragraph [0064], lines 1-4; paragraph [0064], lines 8-10) initiate attestation and establish the requirements for the attestation information transferred between the entities. (see Yan paragraph [0064],

lines 1-17: initial attestation transmitted via message flow between trustor and trustee to establish trust relationship; Yan discloses a two step process for attestation messages (message flows 302, 304 and message flows 306, 308))

The can-attest and attestation-wanted (request, response) messages are used as an attestation initiation protocol sequence. The Yan prior art discloses the initiation of a trust relation between two entities or the initiation of attestation using a two step process as discloses above.

Prior Responses:

3.3 Yan prior art discloses that the first entity has the capability to store multiple versions of the identification information (code ID, integrity metric) for multiple versions of the information for the first entity. (see Yan paragraph [0054], lines 1-14: particular metric may change with time requiring a new value to be stored; provides a way to store sequences of integrity metrics; values of integrity metrics are appended to a sequence)

Yan prior art discloses the capability for the second entity to "know" the first entity when the attestation message is received. Yan prior art checks a list of trusted application as a security or trust check for the attestation message. Yan prior art discloses that the first entity has the capability to store multiple versions of the identification information (code ID, integrity metric) for multiple versions of the information for the first entity.

Yan prior art discloses the additional feature of conditional trust. Yan prior art

discloses the capability to monitor the state of trust between two entities. If the trusted condition changes, appropriate action is taken. Additional features disclosed within a referenced prior art do not remove the fact that the prior art discloses the claim limitation. The Yan prior art discloses the initiation and usage of attestation between two entities in a trusted state. There is no disclosure that the trust solution of the claimed invention does not require a generation of a distrust signal as stated in remarks. The claimed invention makes no mention of a distrust signal. Applicants' remarks state that, "claim 1 is directed towards obtaining a trust-based relationship which does not require a generation of distrust signals for maintaining trust". This is no mention in claim 1 of "distrust signals" or "maintaining trust" without distrust signals in the claimed invention.

The Yan prior art discloses a integrity metric such as a public key, which is used as an identity for the trusted platform. (see Yan paragraph [0055], lines 6-14: trusted platform identity (code ID)) The public key is a value by which the trusted platform is known and is representative of the trusted platform. Other entities have knowledge of the public key. (see specification paragraph [0005] for code ID)

The Yan prior art discloses a symmetric key, (see Yan paragraph [0062], lines 1-4; paragraph [0064], lines 1-4: symmetric key (session key or single key used for cryptographic procedures)), and a public/private key pair (see Yan paragraph [0055], lines 6-14; paragraph [0059], lines 1-12: public/private key pair and certificates) and accompanying certificates.

The Yan prior art discloses attestation initiation. The can-attest and attestation-wanted messages are an attestation initiation sequence protocol. The Yan prior art discloses the initiation of a trust relation between two entities or the initiation of attestation. (Yan paragraph [0058], lines 1-7; paragraph [0060], lines 1-6; paragraph [0060], lines 6-9: initiation of attestation and trust relationship)

Qui prior art does not discredit or discourage the usage of expiration time limits therefore, the Qui prior art does not teach away from the use of expiration time limits. The Qui prior art mentions the difficulties of operating with expiration time limits.

The Qui prior art states:

> (1): "Therefore, restricting certificate lifetime could be used to control the extent of older technology in circulation and to reduce the risk associated with older products being more susceptible to attack" (see Qui paragraph [0021]); and
>
> (2): "However, the shorter lifetime is defined, the more often certificate renewal or re-enrollment would need to be performed, which would increase the operational cost of a certificate authority." (see Qui paragraph [0021])

Statement 1 is an advantage and Statement 2 is a disadvantage. There is no disclosure of teaching away but the mention of alternatives. The mentioning of alternatives is not teaching away.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims **2 - 4, 7 - 12, 14, 18 - 21, 23, 25 - 27, 29, 31** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Yan et al.** (US PGPUB No. **20050033987**) in view of **Qui** (US PGPUB No. **20040148505**).

Regarding Claim 31, Yan discloses a method of establishing trust between two computer entities, the method comprising:

a) transmitting an attestation message from a first computer entity to a second computer entity, the attestation message including a code identifier (code ID) that is calculated by using a security ID corresponding to a behavior parameter that is associated with a computing operation having security implications; (see Yan paragraph [0064], lines 1-17: initial attestation transmitted via message flow between trustor and trustee to establish trust relationship; Yan discloses a two step process for attestation messages (message flows 302, 304 and message flows 306, 308))

Furthermore, Yan discloses:

b) verifying the validity of the code ID in the second computer entity, thereby ensuring that the security ID corresponding to the behavior parameter has not been tampered with; and transmitting a trust message from the second computer entity to the first computer entity upon successfully verifying the validity of the code ID, the trust message including a first secret that is shared between the first

and the second computer entities for communicating securely. (see Yan paragraph [0060], lines 6-9: verify signature, attestation information; paragraph [0062], lines 1-4; paragraph [0064], lines 1-4: session key exchanged between entities for future messaging, communications)

Yan does not specifically disclose a period time whereby a secret is valid. However, Qui discloses a first period of time, wherein the first period of time is determined by the second computer entity. (see Qui paragraph [0040], lines 1-7; paragraph [0021], lines 8-11: expiration timer for certificate information)

It would have been obvious to one of ordinary skill in the art to modify Yan for a period time whereby a secret is valid as taught by Qui. One of ordinary skill in the art would have been motivated to employ the teachings of Qui in order to enable the capability for the generation, transmission, and updating of certificate information when the number of devices is large. (see Qui paragraph [0007], lines 7-12)

Regarding Claims 2, Yan discloses the method of claim 31 wherein the first computer entity encrypts the code ID of the attestation message according to a key available to the second computer entity, the method further comprising the second computer entity decrypting such encrypted matter. (see Yan paragraph [0059], lines 6-12: certificate (public/private) key available to second entity, utilized to encrypt (signature) attestation information)

Regarding Claims 3, Yan discloses the method of claim 31 wherein the second

computer entity consumes the attestation message by application of same to a verifying function that automatically verifies the attestation message based on a format thereof and that extracts relevant information from such verified attestation message for use by the second computer entity. (see Yan paragraph [0060], lines 6-9: verify attestation message with extracted information based on formatted information (certificate information, encrypted hash))

Regarding Claims 4, Yan discloses the method of claim 1 wherein the first computer entity is a part of a computing device, and the second computer entity decides based on the code ID in the attestation message whether the first computer entity can be trusted, and also decides based on a certificate chain of the message whether the computing device can be trusted, the certificate chain leading back to a trusted root authority. (see Yan paragraph [0060], lines 9-12: entity can be trusted; paragraph [0060], lines 1-6: certificate chain utilized to establish trust)

Regarding Claims 7, Yan discloses the method of claim 4 wherein the second computer entity determines that the code ID is a known code ID and that the first computer entity can be trusted based on such code ID. (see Yan paragraph [0060], lines 6-9: check first entity on application trust list based on integrity metric (code ID) of first entity)

Regarding Claims 8, Yan discloses the method of claim 4 wherein the second computer entity determines from the certificate chain whether the computing device of

the first computer entity should be trusted to instantiate and operate the first computer entity in a trusted manner and should be trusted to calculate the code ID properly. (see Yan paragraph [0060], lines 1-9: certificate information utilized to determine trust status)

Regarding Claims 9, Yan discloses the method of claim 8 wherein the second computer entity determines that each certificate in the certificate chain is not on a do-not-trust list. (see Yan paragraph [0060], lines 6-9: check certificate in certificate chain, not on revoked list (do-not-trust list))

Regarding Claims 10, Yan discloses the method of claim 31 wherein the trust message includes a symmetric key (K) that the first and second computer entities shall each employ to encrypt and decrypt messages therebetween. (see Yan paragraph [0062], lines 1-4; paragraph [0064], lines 1-4: session key exchanged between entities for future messaging)

Regarding Claims 11, Yan discloses the method of claim 10 wherein the symmetric key (K) is encrypted according to a public key of the first entity (PU-1) to result in (PU-1(K)), the second entity obtaining (PU-1) from the certificate chain of the attestation message, and wherein the first computer entity obtains the symmetric key (K) from the received trust message by applying a private key (PR-1) corresponding to (PU-1) to (PU-1(K)) to result in (K). (see Yan paragraph [0059], lines 6-12: public/private certificate key, encrypt (signature) attestation information)

Regarding Claims 12, Yan discloses the method of claim 31 wherein the trust message further includes an identification of a cryptographic algorithm to be employed in connection with the first secret. (see Yan paragraph [0062], lines 1-4; paragraph [0064], lines 1-4: session key for secure communications (interaction); paragraph [0065], lines 9-15: updated attestation information (cryptographic algorithm), protocol for exchange negotiated)

Regarding Claims 14, Yan discloses the method of claim 1 wherein the trust message further includes relevant trust data encrypted according to a key available to the first computer entity, and wherein the first computer entity decrypts the encrypted trust data by applying the key thereto. (see Yan paragraph [0059], lines 6-12: public/private key certificate (available to first entity) used to encrypt (signature) attestation information)

Regarding Claims 18, Yan discloses the method of claim 1 wherein prior to the first computer entity transmitting the attestation message, the first computer entity sends a can-attest message to the second computer entity, the can-attest message stating that the first computer entity can send an attestation message but that the first computer entity would like to know from the second computer entity whether such an attestation message is required by such second computer entity and if so any requirements that such second computer entity has with regard to such attestation message, the method further comprising the second computer entity sending an attestation-wanted message

to the first computer entity in response to the can-attest message, the attestation-wanted message stating that the second computer entity does in fact require an attestation message from the first computer entity and that the attestation message as sent by the first computer entity must adhere to certain requirements as defined in such attestation-wanted message, whereby the first computer entity thereafter sends the attestation message in accordance with the requirements stated in the attestation-wanted message. (see Yan paragraph [0064], lines 1-17: initial attestation transmitted via message flow between trustor and trustee to establish trust relationship; Yan discloses a two step process for attestation messages (message flows 302, 304 and message flows 306, 308)); paragraph [0065], lines 9-15: update attestation (wanted-message) information, negotiate protocol for exchange of attestation information)

Regarding Claims 19, Yan discloses the method of claim 30 further comprising:

a) the first computer entity constructing, in accordance with the requirements stated in the attestation-wanted message, the attestation message to be delivered to the second computer entity, the attestation message including a code identifier (code ID) representative of the first computer entity and data relevant to the purpose of the trust-based relationship; (see Yan paragraph [0064], lines 1-17: initial attestation transmitted via message flow between trustor and trustee to establish trust relationship; Yan discloses a two step process for attestation messages (message flows 302, 304 and message flows 306, 308); paragraph [0060], lines 6-9: check entity integrity metric (code ID), identify on application

trust list)

Furthermore, Yan discloses the following:

b) the first computer entity appending a digital signature to the attestation message and a certificate chain leading back to a trusted root authority, the signature being based on the code ID and data thereof and being verifiable based on a security key included in the certificate chain, the certificate chain including at least one certificate therein proffering trustworthiness of the first computer entity; (see Yan paragraph [0060], lines 1-6: certificate chain utilized for attestation information, (exchange, verification))

c) the first entity sending the attestation message to the second entity and the second entity receiving same, whereby the second entity verifies the signature of the received attestation message based on the included security key (see Yan paragraph [0060], lines 6-9: verify signature, attestation information), whereby alteration of the code ID or data of the attestation message should cause the signature to fail to verify, the second entity based on such a failure dishonoring such attestation message, the second entity decides whether to in fact enter into the trust-based relationship with the first entity based on the code ID and the data in the attestation message, the second entity upon deciding to in fact enter into the trust-based relationship with the first entity constructs a trust message to be delivered to the first entity, the trust message establishing the trust-based relationship and including therein a secret to be shared between the first and second entities, where such shared secret allows such first and second entities

to communicate in a secure manner, and the second entity sends the trust message to the first entity and the first entity receiving same; (see Yan paragraph [0062], lines 1-4; paragraph [0064], lines 1-4: session key exchanged between entities for future messaging, communications; paragraph [0060], lines 6-9: check entity integrity metric (code ID), identify on application trust list)

d) the first entity obtaining the shared secret in the trust message and employing the shared secret to exchange information with the second entity according to the established trust-based relationship with such second entity. (see Yan paragraph [0062], lines 1-4; paragraph [0064], lines 1-4: session key exchanged between entities for future messaging, communications)

Regarding Claims 20, Yan discloses the method of claim 19 wherein the code identifier (code ID) is calculated from the digest of the first computer entity, whereby alteration of the first computer entity causes the code ID to change. (see Yan paragraph [0065], lines 9-15: updated integrity metric (code ID) modified, new attestation protocol required)

Regarding Claims 21, Yan discloses the method of claim 20 wherein the code identifier (code ID) is calculated from the digest of the first computer entity and from security information relating thereto, whereby alteration of the first computer entity or the security information causes the code ID to change. (see Yan paragraph [0065], lines 9-15: alteration of security information causes integrity metric (code ID) to be modified)

Regarding Claims 23, Yan discloses the method of claim 19 further comprising a code ID calculator of the first computer entity that is used for calculating the code ID, the code ID calculator operating in a trusted manner in a computing device. (see Yan paragraph [0020], lines 7-8: generate integrity metric (code ID) on trusted device)

Regarding Claims 25, Yan discloses the method of claim 19 wherein the first computer entity creates the attestation message by application of the code ID and data thereof to a quoting function that automatically produces the attestation message in an appropriate format that is accessible to the second computer entity. (see Yan paragraph [0065], lines 9-15: attestation information generated in an accessible format (negotiated) with second entity))

Regarding Claims 26, Yan discloses the method of claim 19 wherein the second computer entity constructs a trust message including therein a shared secret comprising a symmetric key (K) that the first and second computer entities employ to encrypt and decrypt messages therebetween, the symmetric key (K) being encrypted according to a public key (PU-1) to result in (PU-1(K)), the second entity obtaining (PU-1) from the certificate chain of the attestation message, the method comprising the first entity obtaining the symmetric key (K) from the received trust message by applying a private key (PR-1) corresponding to (PU-1) to (PU-1(K)) to result in (K). (see Yan paragraph [0062], lines 1-4; paragraph [0064], lines 1-4: session key utilized for messaging

between first and second entities; paragraph [0059], lines 4-9: public/private key for encryption/decryption (signature attachment))

Regarding Claims 27, Yan discloses the method of claim 19 wherein the second computer entity constructs a trust message further including relevant trust data encrypted according to a key available to the first computer entity, the method comprising the first computer entity decrypting the encrypted trust data by applying the key thereto. (see Yan paragraph [0059], lines 6-12: attestation information encrypted (signature) based on public/private keys (known to first entity))

Regarding Claims 29, Yan discloses the method of claim 19 whereby the trust message is a first trust message and the shared secret is a first shared secret, and whereby the second computer entity constructs a second trust message to be delivered to the first computer entity, the second trust message including therein a second secret to be shared between the first and second computer entities, where such second shared secret allows such first and second computer entities to communicate in a secure manner (see Yan paragraph [0062], lines 1-4; paragraph [0064] lines 1-4: session key exchanged between entities for future messaging), and the second computer entity sends the second trust message to the first computer entity and the first computer entity receives same, the method further comprising the first computer entity obtaining the second shared secret in the trust message and employing the second shared secret to exchange information with the second computer entity, whereby the

first shared secret is no longer valid. (see Yan paragraph [0065], lines 9-15: update attestation information, previous attestation information invalid)

Regarding Claim 32, Yan discloses the method of claim 31, wherein the security ID is stored in a location in the first computer entity, and wherein the first computer entity is constrained to executing a particular behavior only via accessing the stored location. (see Yan paragraph [0040], lines 10-13: provides a facility whereby a platform may store secrets accessible only when platform is in a defined configuration)

Regarding Claim 33, Yan discloses the method of claim 31, wherein the behavior parameter comprises opening of a file in the first computer entity. (see Yan paragraph [0054], lines 1-14: metrics that reflect configuration state; a metric may change with time, this requiring a new value to be stored; specification paragraph [0027] discloses opening and reading a file used to modify security environment)

Regarding Claim 34, Yan discloses the method of claim 31, wherein the behavior parameter comprises opening a debugging port in the first computer entity. (see Yan paragraph [0054], lines 1-14: metrics that reflect configuration state; a metric may change with time, this requiring a new value to be stored; specification paragraph [0027] discloses debugging port used to modify security environment)

Regarding Claim 35, Yan discloses the method of claim 31, wherein the trust

message. (see Yan paragraph [0017], lines 1-6: establishing and maintaining trust between a trustee and a trustor; generating metrics of a trustor and comparing to current metrics of a trustee) Yan does not specifically disclose a period time whereby a secret is valid. However, Qui further discloses data to inform the first computer entity of the first period of time over which the first secret is valid. (see Qui paragraph [0040], lines 1-7; paragraph [0021], lines 8-11: expiration timer for certificate information)

It would have been obvious to one of ordinary skill in the art to modify Yan for a period time whereby a secret is valid as taught by Qui. One of ordinary skill in the art would have been motivated to employ the teachings of Qui for the generation, transmission, and updating of certificate information when the number of devices is large. (see Qui paragraph [0007], lines 7-12)

Regarding Claim 36, Yan discloses the method of claim 31, further comprising: retransmitting the trust message from the second computer entity to the first computer entity, the retransmitted trust message including a) a second secret that is different than the first secret,

Yan does not specifically disclose a period time whereby a secret is valid. However, Qui further discloses data to inform the first computer entity of a second period of time over which the second secret is valid. (see Qui paragraph [0040], lines 1-7; paragraph [0021], lines 8-11: expiration timer for certificate information)

It would have been obvious to one of ordinary skill in the art to modify Yan to enable the capability for a trust message further including an expiration time as taught

by Qui. One of ordinary skill in the art would have been motivated to employ the teachings of Qui for the generation, transmission, and updating of certificate information when the number of devices is large. (see Qui paragraph [0007], lines 7-12)

6. Claims **16, 28** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Yan** in view of **Grawrock** (US PGPUB No. **20040117625**).

Regarding Claims 16, Yan discloses the method of claim 31 wherein the second computer entity creates the trust message by application of that automatically produces the trust message in an appropriate format that is accessible to the first computer entity. (see Yan paragraph [0059], lines 6-12: generate formatted attestation information)
Yan does not specifically disclose a sealing function.
However, Grawrock discloses wherein a sealing function. (see Grawrock paragraph [0018], lines 12-16; paragraph [0025], lines 1-7; paragraph [0026], lines 1-6: seal/unseal trusted operation utilized)

It would have been obvious to one of ordinary skill in the art to modify Yan to enable the capability to perform a seal operation as taught by Grawrock. One of ordinary skill in the art would have been motivated to employ the teachings of Grawrock to provide local users and remote computing devices an efficient and easier method for the completion of trusted operations. (see Grawrock paragraph [0002], lines 7-14)

Regarding Claims 28, Yan discloses the method of claim 19 wherein the first computer entity consumes the trust message by application of same that automatically extracts

the shared secret and other relevant information from such trust attestation message for use by the first computer entity. (see Yan paragraph [0060], lines 6-9: extracts attestation information for processing)

Yan does not specifically disclose whereby an unsealing function.

However, Grawrock discloses wherein an unsealing function. (see Grawrock paragraph [0018], lines 12-16; paragraph [0025], lines 1-7; paragraph [0026], lines 1-6: seal/unseal trusted operation utilized)

It would have been obvious to one of ordinary skill in the art to modify Yan to enable the capability to perform an unseal operation within a trusted computing environment as taught by Grawrock. One of ordinary skill in the art would have been motivated to employ the teachings of Grawrock to provide local users and remote computing devices an efficient and easier method for the completion of trusted operations. (see Grawrock paragraph [0002], lines 7-14)

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless -
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

8. Claim **30** is rejected under 35 U.S.C. 102(e) as being anticipated by **Yan et al.** (US PGPUB No. **20050033987**).

Regarding Claims 30, Yan discloses a method of establishing trust between a first computer entity and a second computer entity, the method comprising: first computer entity constructing the attestation message, the first computer entity sending a can-attest message to the second computer entity, the can-attest message stating that the first computer entity can send an attestation message but that the first computer entity would like to know from the second computer entity whether such an attestation message is required by such second computer entity and if so any requirements that such second computer entity has with regard to such attestation message, whereby the second computer entity sends an attestation-wanted message to the first computer entity in response to the can-attest message, the attestation-wanted message stating that the second computer entity does in fact require an attestation message from the first computer entity and that the attestation message as sent by the first computer entity must adhere to certain requirements as defined in such attestation-wanted message, the first computer entity thereafter sending the attestation message in accordance with the requirements stated in the attestation-wanted message. (see Yan paragraph [0064], lines 1-17: initial attestation transmitted via message flow between trustor and trustee to establish trust relationship; Yan discloses a two step process for attestation messages (message flows 302, 304 and message flows 306, 308))

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to CARLTON V. JOHNSON whose telephone number is (571)270-1032. The examiner can normally be reached on Monday thru Friday , 8:00 - 5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2436

Carlton V. Johnson
Examiner
Art Unit 2436

CVJ
July 6, 2009